Technology

Think Before You Click — or Pay the Price: How to Prevent Ransomware Attacks

BY DANIEL J. SIEGEL

Electronic filing has made the lives of lawyers and their staff much easier. The traditional 5 p.m. or earlier deadlines do not exist, there is no need to print and serve most filings upon other counsel, and even when physical copies are required, the number of copies is generally fewer than the number required in the old days; that is, before the advent of e-filing.

But it is not only e-filing that has made lawyers' lives easier. It is the easy access to other information, from real property records to dockets, that also allows users to get more done more efficiently than ever.

So when a court or governmental website goes offline, users bemoan the complications that arise. For example, when the Philadelphia courts went offline on May 21, 2019, my office was involved in a case where we had filed a Motion for Summary Judgment the day before. The Motion with exhibits was over 1,000 pages. We thanked God that we did not have to print out and mail the Motion to the seven other firms involved in the case.

Philadelphia's outage lasted until July 2019. Thus, the opposing party in our case was not so lucky. They were forced to cart over their Response, which contained as many, or perhaps more, pages than did our Motion. Their hassle and increased expense was palpable.

In late 2020, Delaware County experienced a similar outage, which not only included the courts, but also the majority of county electronic services. Again, the impact was substantial on lawyers and the public.

The cause of Philadelphia's outage was never disclosed, although many observers believe that it arose because the site had been hacked. Delaware County admitted it was the subject of a ransomware attack, and that it paid $25,000 to rescue its data. Compared with the reported cost of many ransomware attacks, Delaware County got off cheap and, the county website was back online quickly. Still, as with the Philadelphia outage, users lamented that they suddenly were forced to print and file paper copies of documents, and were unable to view the dockets in their cases.

These types of attacks are common, and they should serve as a chilling wakeup call to lawyers. According to the cyber-insurance provider Coalition, 41 percent of all cyberinsurance claims in the first six months of 2020 were related to ransomware attacks. More troubling is the fact that the primary cause of these ransomware attacks was "exploitation of remote access," *i.e.*, users clicking on links in spam or phishing emails.

In other words, the number one cause of ransomware attacks is user error or ignorance, not proactive efforts by cyberhackers. Thus, in most cases the weakest link was staff.

Ransomware is simply software that gains access to computer files or systems, and then blocks users from accessing their files or systems. As a result, all files, including those on devices that access the system, are held hostage until the victim pays ransom to the hacker in exchange for receiving the decryption key, *i.e.*, the code that unlocks the subject files or systems.

Fortunately, it is relatively easy to prevent ransomware attacks, with user training being the first and most important line of

defense. In most cases, firms hire outside trainers to educate staff. There are also excellent guides that explain how to prevent a ransomware attack. For example, global technology company Cisco offers a free special edition of *Ransomware Defense for Dummies*, which is available at http://bit.ly/CiscoRansomwareBook, and is an excellent introductory guide to understanding and preventing ransomware attacks.

Most cybersecurity experts agree that by taking the following precautions, you can prevent most ransomware attacks:

Never click on links in email unless you are absolutely certain they are valid.
Do not click on links in spam emails. And remember, not all spam emails look like spam. Hackers can "spoof" email addresses fairly easily. If an email message or format does not seem quite right, or your inner "alarm" is going off, instead of clicking, hover your mouse over the link and if the address that displays is one that you are not familiar with, do not click on it. If you are not sure that the link is valid, contact the sender by sending a separate email (do not forward the potential spam) and asking whether they were the source of the email. Clicking on these forms of malicious links is the number one way computers get infected, not only with ransomware, but also all forms of viruses.

Do not open untrusted email attachments.
Do not click on attachments to email unless you are certain that the email came from a source you know and trust. If you are not sure that the attachment is safe, contact the sender by sending a separate email (do not forward the potential spam) and asking whether they were the source of the email.

Only download files from websites you trust.
You would not let your children eat candy unless they were given it by someone you know and trust. Similarly, you should not download anything from websites you do not know and trust. Trusted websites will generally have "https" at the start of their URL/website address. There may also be a shield or padlock symbol in the address bar.

Do not give out personal data.
Do not give out personal information if you receive an email from an unknown or untrusted source. Similarly, do not give out this information in response to a text or phone call.

Keep your software up-to-date.
In my last column, I discussed the danger of using outdated or unsupported software. Always keep your software up-to-date and do not use software that is no longer supported or updated, such as Windows XP. Cyberhackers try to gain access by looking for vulnerable software; do not help them.

Use security software, including antivirus and antimalware products.
These products provide a broad range of protection for computers, including firewalls, antivirus and malware protection, and more. There are many excellent products that are appropriate for solo and small firms. Midsize and larger firms can also benefit from firmwide protection.

PC Magazine, a trusted source of computer information, highly rates security products from the following companies (listed alphabetically):

- Bitdefender Internet Security
- Kaspersky Internet Security
- McAfee Total Protection
- Norton 360 Deluxe
- Trend Micro Maximum Security
- Webroot SecureAnywhere Internet Security Complete

Another source of protection is to purchase cyberinsurance. In general, many of these policies will consider paying the ransom, although it varies by the situation. In general, cyberinsurance is best procured by obtaining a separate policy rather than as a rider to a general liability insurance policy.

There is no doubt that ransomware is a serious problem, which is not going away anytime soon. It pays to take precautions to avoid having to pay the cyberattacker. ■

Daniel J. Siegel, (dan@danieljsiegel.com), a member of the Editorial Board of The Philadelphia Lawyer, is a practicing attorney and the president of Integrated Technology Services LLC, a consulting firm that helps law offices improve their workflow through the use of technology.

Tech BRIEFS

SMOKEBALL

Smokeball is a legal case management software specialized for small law firms. This software is cloud-based and runs on Windows.

SMOKEBALL

Lawyers of any practice can utilize this software to approach legal work with a more confident, accurate, and organized effort. Smokeball automates your workflow by assembling documents, doing calculations, managing due dates and calendars, and overall ensuring your precise representation for all of your clients.

With its automatic time and activity tracking, legal document automation, free unlimited onboarding, and Microsoft Word and Outlook integrations, this software provides you with the resources to comprehensively manage your practice.

Additional Features Include:
1. Client Communication Portal
2. Legal Form Library
3. Billing software – integrates with LawPay, QuickBooks, and more
4. E-Filing and Electronic Signatures Abilities
5. Law Firm Insights – time and performance tracking
6. Unlimited document storage
7. Case management
8. Document assembly assistance

This software program is $39.95 per month.

Demos for this program are available at: https://www.smokeball.com/watch-demo/

Tech UPDATE

** Comparisons sourced from www.pcmag.com*

Altec Lansing Waterproof In-Ear Earbuds

Razer Nari Essential

Jabra Elite Active 75T

CANCEL OUT NOISE AND DISTRACTIONS in style and on the move. With a new pair of wireless earphones, you can concentrate in your home office comfortably. Earphones are water-resistant and can be used in various settings. From morning runs to at-home offices, these affordable wireless headphones will help you thrive in your day-to-day life at home.

	ALTEC LANSING WATERPROOF IN-EAR EARBUDS	RAZER NARI ESSENTIAL	JABRA ELITE ACTIVE 75T
BEST FOR	RUNNING, EXERCISING, AVERAGE EARPHONE NEEDS	GAMING	RUNNING, EXERCISING, AVERAGE EAR-PHONE NEEDS
SIZE / WEIGHT	9MM SPEAKER SIZE	40 MM SPEAKER SIZE; MAJOR INNER-EAR CUP DIAMETER 67 MM, MINOR INNER-EAR CUP DIAMETER 56 MM	6MM SPEAKER SIZE
FEATURES	• 7.1-CHANNEL SURROUND SOUND • RATED IPX7 – CAN BE SUBMERGED IN UP TO 1 METER OF WATER FOR 30 MINUTES. • RESISTANT TO DUST AND SHOCKS • 3 PAIRS OF TIPS INCLUDED IN SMALL, MEDIUM, AND LARGE SIZES • 33 FEET WIRELESS RANGE	• 7.1-CHANNEL SURROUND SOUND • BATTERY LIFE UP TO 16 HOURS • CONNECT THROUGH A WIRELESS USB TRANSCEIVER; USB TRANSMITTER INCLUDED • BENDABLE UNIDIRECTIONAL MICROPHONE	• 6MM DRIVER IN EACH EAR DELIVERS A FREQUENCY RANGE OF 20HZ TO 20KHZ • IP RATING FROM 56 TO 57 FOR WATER-RESISTANCE UP TO 1 METER • 7.5 HOURS BATTERY LIFE • CHARGING CASE CAN EXTEND THE ELITE ACTIVE'S BATTERY LIFE TO UP TO 28 HOURS • CHARGING VIA USB-C AND USE BLUETOOTH 5.0
PROS	• STRONG BASS AND NO DISTORTION • RUGGED, WATERPROOF DESIGN • A CARRYING POUCH INCLUDED • BUDGET-FRIENDLY	• POWERFUL SOUND • STURDY, COMFORTABLE DESIGN • USER-ADJUSTABLE EQ • EXCELLENT MIC	• BATTERY BOOST • SMALLER FRAME • EXTRA DUST- AND SWEAT-RESISTANCE
CONS	• AVERAGE SOUND QUALITY • COULD BE MORE COMFORTABLE	• HEAVY ON BASS BY DEFAULT • 7.1-CHANNEL SURROUND AND EQ TWEAKS ARE ONLY AVAILABLE ON PC	• SCULPTED SOUND SIGNATURE MIGHT BE TOO MUCH FOR SOME • EXPENSIVE
PRICE	$29.99	$99.99	$199

PHILADELPHIA BAR ASSOCIATION

Lawyer Referral and Information Service

(215) 238-6333 | PhiladelphiaBarLawyers.com

TRUST US TO HELP

LRIS Has Been Helping the Community Since 1948

- LRIS refers potential clients to approximately 175 attorneys.
- LRIS attorneys are in good standing, have professional liability insurance and must meet certain experience requirements.
- LRIS attorneys practice in more than 150 areas of law.
- In 2017, LRIS received 25,425 inquiries and made 11,208 referrals.

If You Have Someone You Cannot Help… Refer Them to Us!

Questions?

For questions, contact Director of Public and Legal Services Charlie Klitsch at (215) 238-6326 or cklitsch@philabar.org.

Lawyer Referral and Information Service of the Philadelphia Bar Association
1101 Market St., 11th Floor
Philadelphia, PA 19107